

What is claimed is:

1. A system, comprising:

a plurality of collector devices that are disposed to
collect statistical information on packets that are sent between
5 nodes on a network;

an aggregator that receives network data from the plurality
of collector devices, and which produces a connection table that
maps each node on the network to a record that stores
information about traffic to or from the node.

10 2. The system of claim 1 wherein the aggregator
determines occurrences of network events.

3. The system of claim 2 wherein the aggregator further
comprises:

a process that communicates occurrences of network events
15 to an operator.

4. The system of claim 1 wherein the aggregator device
further comprises:

a process to aggregate anomalies into the network events.

5. The system of claim 1 wherein the collectors have a
20 passive link to devices in the network.

6. The system of claim 1 wherein the anomalies include
denial of service attacks and scanning attacks.

7. The system of claim 1 wherein the anomalies include
unauthorized access and worm propagation.

8. The system of claim 1 wherein the connection table includes a plurality of records that are indexed by source address.

5 9. The system of claim 1 wherein the connection table includes a plurality of records that are indexed by destination address.

10. The system of claim 1 wherein the connection table includes a plurality of records that are indexed by time.

10 11. The system of claim 1 wherein the connection table includes a plurality of records that are indexed by source address, destination address and time.

12. The system of claim 1 wherein the connection table includes a plurality of connection sub-tables to track data at different time scales.

15 13. The system of claim 1 wherein the connection sub-tables include a time-slice connection table that operates on a small unit of time and at least one other sub-table that operates on a larger unit of time than the time slice sub-table with each sub-table holding the sum of records received from all
20 collectors during respective units of time.

14. A method, comprises:
providing a plurality of collector devices in a network to collect statistical information on packets that are sent between nodes on a network; and

sending statistical information from the collector devices to an aggregator, the aggregator producing a connection table that maps each node on the network to a record that stores information about traffic to or from the node.

5 15. The method of claim 14 wherein the aggregator determines occurrences of network events.

16. The method of claim 15 further comprises:
aggregating anomalies into the network events and
communicating occurrences of network events to an operator.

10 17. The method of claim 14 wherein the connection table includes a plurality of entries that are indexed by source address.

15 18. The method of claim 14 wherein the connection table includes a plurality of entries that are indexed by destination address.

19. The method of claim 14 wherein the connection table includes a plurality of records that are indexed by time.

20 20. The method of claim 14 wherein the connection table includes a plurality of records that are indexed by source address, destination address and time.

21. The method of claim 14 wherein the connection table includes a plurality of connection sub-tables to track data at different time scales.

25 22. The method of claim 14 wherein the connection sub-tables include a time-slice connection table that operates on a

small unit of time and at least one other sub-table that operates on a larger unit of time than the time slice sub-table with each sub-table holding the sum of records received from all collectors during respective units of time.

5 23. A method of detecting a new host connecting to a network comprises:

 receiving statistics collected from a host in the network;
and

 indicating to a console that the host is a new host if,
10 during a period of time T, the host transmits at least N packets and receives at least N packets, and if the host had never transmitted and received more than N packets in any previous period of time with a duration of T.

 24. A method of detecting a failed host in a network
15 comprises:

 determining if both a mean historical rate of server response packets from a host is greater than M, and a ratio of a standard deviation of historical rate of server response packets from the host to a mean profiled rate of server response packets
20 from the host is less than R over a period of time; and

 indicating the host as a potential failed host if both conditions are present.